Data associations and the protection of reputation online in Australia

Joyce, Daniel

2017-05-29

Joyce , D 2017 , ' Data associations and the protection of reputation online in Australia ' , Big Data & Society , vol. 4 , no. 1 , pp. 1-10 . https://doi.org/10.1177/2053951717709829

http://hdl.handle.net/10138/232602
https://doi.org/10.1177/2053951717709829

Original Research Article

BIG DATA & SOCIETY

Big Data & Society
January–June 2017: 1–10

DOI: 10.1177/2053951717709829
journals.sagepub.com/home/bds
SAGE

Data associations and the protection of reputation online in Australia

Daniel Joyce

Abstract

This article focuses upon defamation law in Australia and its struggles to adjust to the digital landscape, to illustrate the broader challenges involved in the governance and regulation of data associations. In many instances, online publication will be treated by the courts in a similar fashion to traditional forms of publication. What is more contentious is the question of who, if anyone, should bear the responsibility for digital forms of defamatory publication which result not from an individual author's activity online but rather from algorithmic associations. This article seeks, in part, to analyse this question, by reference to the Australian case law and associated scholarship regarding search engine liability. Reflecting on the tensions involved here offers us a fresh perspective on defamation law through the conceptual lens of data associations. Here the focus of the article shifts to explore some wider questions posed for defamation law by big data. Defamation law may come to play a significant role in emerging frameworks for algorithmic accountability, but these developments also call into question many of its traditional concepts and assumptions. It may be time to think differently about defamation and to consider its interrelationship with privacy, speech and data protection more fully. As a result, I conclude that the courts and policymakers need to engage more deeply and explicitly with the rationale(s) for the protection of reputation and that more thought needs to be given to changing conceptions of reputation in the context of data associations.

Keywords

Data associations, automaticity, algorithms, search engines, defamation law, reputation

Introduction

This article has resulted from an invitation to think about the protection of reputation as an element of a broader framework for the governance of data associations. It draws upon some recent case law in Australia to trigger wider reflection about the need for defamation law (in a variety of contexts) to engage with the theme of data associations. It is in this sense a reflective piece rather than a doctrinal analysis. I approach defamation law not as a private lawyer, but from the perspective of media law and its current entanglement with the digital. Defamation law scholarship, much of it doctrinal and private law focused, is beginning to engage more fully with comparative law and with questions of jurisdiction in the private international law sense, and it is also productive to begin to think about this subject from the perspective of data, big data and data protection. This article is written in the spirit of such enquiry.

The article begins, in the first section, by contextualising the broader theme of data associations in light of Australian defamation law's response to the varied challenges of the Internet. The discussion then moves, in the second section, to explore a few contemporary cases illustrating some of the conceptual problems involved by reference to the specific problem of search engine liability. Search engine liability is a current concern in the case law and for my purposes it offers a useful illustration of defamatory matter potentially arising as a result of data associations, where defamatory matter is connected with an individual

UNSW Sydney, Australia; Australian Human Rights Centre, Australia; University of Helsinki, Helsinki, Finland

Corresponding author:
Daniel Joyce, Faculty of Law, UNSW Sydney, NSW 2052, Australia.
Email: daniel.joyce@unsw.edu.au

through the operation of an algorithm. It is not my intention to definitively set out legal doctrine in this shifting area. I use the case law as illustration of broader difficulties faced by the courts in grappling with data associations and because I think it is useful to think differently about defamation law.

This prompts deeper reflection in the third section. Have the cases tended to focus on complex questions regarding publication and jurisdiction to the detriment of other equally important areas such as identification and meaning? Does the theme of data associations draw these other elements of the cause of action more fully into view? Building on this conceptual reflection, and prompted by earlier analysis of the case law regarding data associations, the fourth section reflects more broadly upon the challenge offered by big data to defamation law. Do defamatory data associations, as in the case of search engines, provide a new way of thinking about the protection of reputation and the traditional principles of defamation law? Here I begin to articulate some new ways of considering the conceptual foundations of the subject. I argue that defamation law is centrally placed within debates over how to develop forms of algorithmic accountability. This potential role, however, prompts the need to address deeper questions within domestic systems of defamation law concerning their underlying rationale(s) and assumptions, and also regarding the interrelationship between defamation law, privacy, speech and data protection. To set the scene for this later discussion of defamation law's engagement with data associations, first I turn to consider how Australian defamation law has struggled with the Internet and then with search engines in particular.

Australian defamation law, online publication and automaticity

The tort of defamation is said to involve the balancing of two key interests – reputation and free speech. In the Australian context, without a bill of rights or more direct constitutional protection for speech, and with no free-standing cause of action for invasion of privacy, defamation law is arguably the dominant area of media law. But it is a costly, esoteric and rather unpredictable vehicle, and many increasingly argue for reform and suggest that in fundamental ways it is no longer fit for task (Descheemaeker, 2009; Rolph, 2016: 1–7).

The rapid development of the Internet along with associated changes occurring in the digital media landscape has challenged and affirmed the principles of media law in a variety of areas, prompting a range of regulatory proposals and responses. We talk of convergence and the need for technology-neutral and converged forms of regulation. There are efforts to embrace de-professionalisation and the rise of citizen media, seeking functional rather than professional privileges and status in order to protect the bloggers. And there are also the reverse, efforts to re-professionalise in the face of change, and to challenge the idea that all with the capacity to publish are 'the media'. Some call for the end of formal regulation – as in the death of privacy. Others argue that we need stricter protection for privacy and better integration of the uneven, and at times conflictual, media law mechanisms (Australian Law Reform Commission, 2014). Some call for a focus on data or information in our media law, so that areas such as privacy protection should come to be seen as 'information rules', or argue that defamation law needs to better take account of data protection jurisprudence (Erdos, 2014). Others see new possibilities for softer forms of self-regulation and reputation management in the digital media landscape, or in ideas such as a right to reply or even a right to be forgotten.

Defamation law has, from its origins, grappled with questions regarding the development of communications technologies – notably the printing press. Recent scholarship and case law has focused on the applicability of defamation law principles in an online environment, but to date little has been said explicitly about data and defamation, though this has become an important theme for privacy scholarship.

Here I define data simply as information in digital form, thus capturing all forms of digital media and online publication. Computing allows algorithmic analysis of massive sets of data – commonly referred to as 'big data'. This results in increasing power and influence being wielded by companies involved in the information economy and in developing tools for algorithmic data association and the collation and commodification of big data sets. As Frank Pasquale (2015a: 8) argues: 'authority is increasingly expressed algorithmically. Decisions that used to be based on human reflection are now made automatically'. Pasquale (2015a: 59) argues of the companies like Google Inc, which have developed the dominant mechanisms of search: 'These new masters of media are more than just conveniences. Thanks both to their competence and our inertia, they often determine what possibilities reach our awareness at all'. For defamation law, the Internet and the accessibility of self-publication, searchability, increased interactivity and citizen-generated content have prompted a degree of soul-searching. Should these developments call traditional defamation law principles into question? There is a certain 'shock of the new' excitement about the application of defamation law to green fields, which blends with the reformist emphasis in much of contemporary defamation law scholarship. But on closer inspection defamation law's principles, at least in Australia, remain fairly intact.

This can be seen in one element of the cause of action – publication. Publication has been traditionally construed very broadly. As Isaacs J noted in an early Australian High Court case: '[t]o publish a libel is to convey by some means to the mind of another the defamatory sense embodied in the vehicle' (*Webb v Bloch*, 1928, at p. 363). Practically everything is a publication – so why not a tweet or indeed a re-tweet or share on Facebook (covered by the principle of repetition)?

Commonly those with control over, who facilitate or assent to, publication can be liable for it as contributing to the publication in the broad sense required. It is in this way that editors, newspaper proprietors and printers traditionally have been held to be publishers along with journalists. But publication can also arise from omission (or authorisation) as in the case of *Byrne v Deane*, which involved failure to take down allegedly defamatory verse posted on a golf club's wall for several days where the club rules provided that no notice or placard shall be posted in the club premises without the consent of the secretary. This line of authority has been relevant in the case of Internet Service Providers and their failure to remove defamatory material but is less applicable in the context of search engines. The policy-based defence of innocent dissemination gives rise to a further category of subordinate distributors (or secondary publishers) such as newsagents and libraries. In certain contexts, the defence will apply where dissemination occurs without knowledge of the defamatory matter published (there is also statutory expression of the defence, for example *Defamation Act* 2005 (NSW), s. 32). This variety in terms of how one can be deemed to have published (or not) defamatory material has resulted in mixed results in the cases and points to the need for fact specificity in consideration of the question of publication as it arises in the context of different kinds of Internet intermediary cases – search engine publication will necessarily be treated differently to Internet Service Provider or platform publications (Rolph, 2016: 162; *Google v Trkulja*, 2016, at [285]). The relevance of notice in determining liability in the latter two categories of publication (*Byrne v Deane* and *Emmens v Pottle*) is apparent, but 'for different reasons' (*Google v Trkulja*, 2016, at [243], [283]).

In terms of how to address the challenge of jurisdiction online, for the Australian courts, every publication gives rise to a separate cause of action (*Dow Jones v Gutnick*). Only the area of defences, such as triviality and innocent dissemination, and consideration of statutory protections for Internet Service Providers and Internet Content Hosts give rise to more ambiguity. And in this area it has been left to the Australian legislature to attempt to reform the law, where currently some provision is made by Clause 91(1), Schedule 5 of the *Broadcasting Services Act* 1992 (Cth). Despite some unsettled areas, the traditional principles regarding publication have proved remarkably resilient, and the defence of innocent dissemination, which protects certain classes of subordinate distributors without knowledge of the defamatory meaning, is the main avenue for digital media defendants to argue their case. Thus, following a review of initial decisions relating to publication and innocent dissemination in the context of the Internet, David Rolph (2010: 563) reflected that 'while internet technologies have brought about a revolution in communications, their impact on defamation law has not been equally radical'. The jurisprudence, however, remains dynamic (Rolph, 2016: 162–166). It also points to the possibility and need for statutory intervention and reform over time.

Yet automaticity has proved difficult for the courts in determining whether algorithmic search engine results constitute defamatory publication through association. An early and influential English case illustrated that automaticity might prove a hurdle for plaintiffs to overcome. The decision indicated that search engine operators could not be held liable for defamatory algorithmic publication or defamation by data association (*Designtechnica*). In the context of the facts of the case, Eady J emphasised the lack of control which Google had over the material available on the Internet and over the terms entered by users of its search engine. Eady J (*Designtechnica*, 2011, at p. 1757 at [50]–[51]) stated:

> When a search is carried out by a web user via the Google search engine it is clear… that there is no human input from the third defendant [Google Inc]. None of its officers or employees take part in the search. It is performed automatically in accordance with computer programmes… It has not authorised or caused the snippet to appear on the user's screen in any meaningful sense. It has merely, by the provision of its search service, played the role of a facilitator.

Eady J concluded that Google as a search engine operator must be treated differently to a website host who can remove offending material more readily. Ultimately then Eady J was unwilling to find that Google was a publisher either in terms of 'authorship or acquiescence' and whether before or after notification (*Designtechnica*, 2011, at pp. 1760, 1773 at [64], [124]).

I now turn to examine some subsequent Australian cases, which have also addressed the issue of defamatory liability in the context of data association in the form of Google's search engine. This case law has drawn upon decisions in comparative contexts such as England and Wales, New Zealand, Hong Kong and Canada. For reasons of economy I do not intend here to address all of those comparative cases (see for example, *A v Google*

New Zealand; *Yeung v Google*) but it has been evident that this is an area where, perhaps due to the novelty and complexity of the issues raised, comparative examples have been of benefit to the courts.

Some contemporary Australian decisions involving the Google search engine

Several contemporary Australian cases involving Google illustrate the potential for divergence in this area. It is increasingly clear that not all Internet contexts, nor indeed all forms of Internet intermediary liability, ought to be treated in similar fashion. The Google search engine itself has given rise to different modes of potential liability for distinct aspects such as the autocomplete function, hyperlinks, snippets and images resulting. Whilst all involve data association of some kind, they may not all constitute publication in terms of defamation law or they may be characterised as different forms of publication. There is also evidence of a shift in approach by some judges towards the capacity of Google to remove defamatory material, and hence a mixed view of whether in fact the data association underlying the search engine is automatic (even passive) or able to be actively controlled and directed.

For example, Beach J of the Supreme Court of Victoria considered the liability of search engines as publishers in an important case, *Trkulja v Google (No 5)*. This case saw Australian law begin to diverge from earlier decisions in England and Wales which had questioned whether it was appropriate for Internet intermediaries to be considered as a publisher (Rolph, 2010: 571–573).

During 2009 material was available on the Internet concerning the plaintiff Mr Trkulja. Images and an article online (relating to an attempt on his life) which came up through a simple Google search for Michael Trkulja connected him with figures in the Melbourne criminal underworld, giving rise to imputations that he was a prominent figure in that underworld, that he was so involved that an attempt on his life had been planned and so on. The defendants Google Inc LLC and Google Australia P/L denied publication and pleaded defences of innocent dissemination at common law and under statute.

A jury found that Trkulja had established an entitlement as to damages against Google Inc in respect of certain of the images suggesting his involvement with the Melbourne criminal underworld. However, Google Inc successfully established the defence of innocent dissemination in relation to the matters arising on the web. Google applied for judgement notwithstanding the jury's verdict by way of a non-obstante application.

Google Inc claimed not to be a publisher in relation to the images. Much was made in argument by counsel for Google Inc about the automaticity of the Google search engine and the possibility for avoidance of responsibility where the role played was passive and that of an intermediary.

Beach J (*Trkulja v Google (No 5)*, 2012, at pp. 13–14 at [18], [20]) found, however, that:

> The jury were entitled to conclude that Google Inc intended to publish the material that its automated systems produced... It was a page of Google Inc's creation – put together as a result of the Google Inc search engine working as it was intended to work by those who wrote the relevant computer programs... If Google Inc's submission was to be accepted then, while this page might on one view be the natural and probable consequence of the material published on the source page from which it is derived, there would be no actual original publisher of this page.

Beach J distinguished earlier decisions, reasserting a broad approach to what might constitute search engine publication. Ultimately in his Honour's view: 'it was open to the jury to conclude that Google Inc was a publisher – even if it did not have notice of the content of the material about which complaint was made' (Beach J in *Trkulja v Google (No 5)*, 2012, at p. 18 at [30]).

A more recent decision in NSW yielded a different result through a focus upon case management and proportionality principles. McCallum J stayed proceedings involving Google Inc as a defendant in the matter of *Bleyer v Google*, in part because the cost would be disproportionate to what was at stake. In that case the plaintiff Mr Bleyer alleged that the search engine generated snippets and hyperlinks which conveyed imputations of criminality, though the pleadings were fairly vague as to the particulars of publication (*Bleyer v Google*, 2014, at [9]–[10]). Google had also acted to remove the offending URLs. Her Honour also noted that:

> One of the difficulties with a defamation claim based on the publication of search results using Google or other search engines is that the relevant audience is necessarily confined to the class of persons who have undertaken a Google search using terms that identify the relevant defamatory web page according to the search engine's algorithms. (McCallum J in *Bleyer v Google*, 2014, at [31])

By finding against the plaintiff on the basis of case management and proportionality reasoning, the position taken by McCallum J in *Bleyer* illustrates a shift away from the approach in *Trkulja (No 5)* and Beach

J's characterisation of Google's search engine, and back towards the earlier English decisions of Eady J, which in a range of contexts (some focused on Internet Service Providers and blogging platforms), emphasised the common law's difficulty with defamation via intermediaries. Her Honour states that:

> ... there is no human input in the application of the Google search engine apart from the creation of the algorithm. I would respectfully disagree with the conclusion reached by Beach J in *Trkulja* that the performance of the function of the algorithm in that circumstance is capable of establishing liability as a publisher at common law. I would adopt the English line of authority to the effect that, at least prior to notification of a complaint... Google Inc cannot be liable as a publisher of the results produced by its search engine. (McCallum J in *Bleyer v Google*, 2014, at [83])

Uncertainty in the Australian common law continues with some cases more recently again adopting a wider view of Google's liability in line with *Trkulja (No 5)*. In *Trkulja v Google* (2015) Google ran arguments that it was not a publisher and that as a search engine it should be immune from suit. Such arguments illustrate the public significance of Google's litigation strategy and see the company playing an important role in attempting to shape the developing law in this area across jurisdictions. Google's arguments were rejected. McDonald J followed the authority in *Trkulja (No 5)*, distinguishing the earlier English decisions like *Designtechnica* and stating that 'Google's primary contention that, as a search engine proprietor it cannot be a publisher (either before or after receiving notice of any alleged defamatory publication) is not supported by any authority' (*Trkulja v Google*, 2015, at [6]). Like Beach J, McDonald J adopted a pragmatic view, concluding that '[e]ither Google is the publisher of the material complained of or there is no publisher at all' (*Trkulja v Google*, 2015, at [17], see also [45]). Google was found to be in control of its search engine results and motivated by 'commercial objectives' (*Trkulja v Google*, 2015, at [46]). The breadth of potential liability articulated in earlier cases like *Webb* and *Thompson* ensured that the defence of innocent dissemination was not available and that liability could stretch to accommodate this case of publication by data association 'even if one has not read the material and therefore can have no intention to publish specific words' (*Trkulja v Google*, 2015, at [49], [59], [75]).

Similar conclusions were reached by Blue J in the South Australian case of *Duffy v Google*. Blue J rejected the argument advanced by Google 'that a defendant can only ever be a publisher if the defendant authorises or accepts responsibility for the publication' (*Duffy v Google*, 2015, at [184]). In *Duffy v Google* automaticity was no bar to liability so long as Google was notified and had been given a reasonable time to respond (*Duffy v Google*, 2015, at [206]–[209]).

Not all the recent authority points in this direction. At the time of writing, *Trkulja v Google* (2015) has been appealed successfully with the potential for the issues to reach the High Court of Australia in due course. In *Google v Trkulja* (2016) the Victorian Court of Appeal again considered the issue of search engine liability and publication, allowing Google's appeal. The decision provides a useful overview of the Australian and comparative case law, emphasising the need for conceptual clarity and fact specificity when approaching the complex questions surrounding defamation and the Internet (*Google v Trkulja*, 2016, at [152], [227]–[231], [285]). Indeed, the Court states that 'to speak of the operation of defamation principles in the context of the Internet is an oversimplification which is apt to mislead' (*Google v Trkulja*, 2016, at [99], see also [152]). Equally the decision points to the need to appreciate the different forms of liability for publication, starting with *Webb v Bloch* with its broad approach of contribution to publication and then distinguishing the *Byrne v Deane* form of publication by omission (or authorisation) and the category of secondary publication associated with *Emmens v Pottle, Thompson* and the development of the defence of innocent dissemination (*Google v Trkulja*, 2016, at [100]–[131]).

In considering and contrasting multiple forms of use of the web, the Court notes that

> the interaction between a user and the Google search engine is quite different to the interaction between a user and Facebook or Twitter or the like... Google neither compiles the search terms nor any webpages or images which are identified in response. (*Google v Trkulja*, 2016, at [177])

Emphasis is placed upon the dynamic and multifaceted operation of Google's algorithm (drawing upon *Google v ACCC*, 2013). Google drew on this in argument also pointing to the ways in which search results and autocomplete predictions are responsive to prior user activity (*Google v Trkulja*, 2016, at [218]).

After a careful analysis of the case law, and rejection of the characterisation of Google's search engine as 'passive', the Court returns to first principles, stating that a search engine is a publisher as 'a participant in a chain of distribution of material' but that it 'should be accounted a secondary publisher' and thereby not caught by the repetition rule (*Google v Trkulja*, 2016, at [348]–[349], [357]). Consequently, a defence of innocent dissemination will be available in the period prior

to notification (*Google v Trkulja*, 2016, at [353], [357]). Arguing that too much attention has been given to intention, the Court notes that ours is 'a world where automated action is becoming, if it is not already, the norm' (*Google v Trkulja*, 2016, at [350]–[351]).

The analysis then turns to the element of defamatory meaning. Given the ubiquity and nature of the Google search engine, the Court finds that 'the plaintiff would have no prospect at all of establishing that the images matter conveyed any of the defamatory imputations relied upon' (*Google v Trkulja*, 2016, at [391]). This builds on earlier analysis of the particular images generated by search and the wide and varied range of persons captured, from underworld figures to police officers, actors and barristers (*Google v Trkulja*, 2016, at [25]). The decision follows *Duffy* in determining 'that autocomplete predictions are incapable of being defamatory' and also due to their responsiveness to past searches (*Google v Trkulja*, 2016, at [393]). The web matter is also found not to have carried the imputations alleged (*Google v Trkulja*, 2016, at [396], [404]).

The Court concludes that the problems raised by search engines are 'acute' and have 'led to conflicting analyses in the common law world' (*Google v Trkulja*, 2016, at [412]). Given the social utility of search and the real possibility for defamatory imputations to arise in context, a pragmatic, fact specific and balanced approach is preferred (*Google v Trkulja*, 2016, at [413]). Any question of immunity, as raised in the appeal, should be 'conferred by legislation' (*Google v Trkulja*, 2016, at [414]).

Defamatory meaning and identification

And so, viewing the protection of reputation through the lens of data association, points not only to questions concerning publication (and jurisdiction), but also to the two remaining elements of the cause of action – defamatory meaning and identification. If we view the matter as being the communication via the indexing of a plaintiff with potentially defamatory content *by association*, then we might ask how seriously are we, or more specifically the ordinary reasonable reader, to take such association? There is authority for this form of associative defamatory meaning, for example, in the English case of *Garbett* where defamatory meaning arose through the juxtaposition of photographs and text, thereby damaging the reputation of an innocent outdoor photographer who was associated with neighbouring text and an image suggestive of his involvement with the showing, taking or exhibition of indecent photos (*Garbett v Hazell, Watson & Viney*).

Traditionally defamation law has allowed for defamatory imputations to arise both on the words themselves taken literally, but also by reading in between the lines, or even by inference when comprehended in the light of extrinsic facts. There are of course limits in terms of how far the courts will allow such inferences to be drawn, but the core idea is that much of our communication involves both direct and indirect forms of association, therefore to require only direct identification or to require the defamatory meaning to be explicit, would miss the nature of our communication and reduce the interpretive nuance required to reductive and overly formalistic terms.

But there is also a desire in appellate decisions to rationalise and to some extent to rein in the complexity of defamation law. Addressing the variance of approaches to what constitutes defamation at common law, a powerful majority of the High Court of Australia in the case of *Chesterton* has stated a general test for defamatory meaning in the following terms:

> The likelihood that the ordinary reasonable person may think the less of a plaintiff because of the imputations is assessed by reference to that person's general knowledge and their knowledge of standards held by the general community, as they may apply to what is said about the plaintiff. Because such a person can be expected to apply the standards of the general community, he or she may be described as ''decent''. The standards are not limited to those of a moral or ethical kind. (*Radio 2UE Sydney P/L v Chesterton*, 2009, at p. 484)

The scholarly work of Lawrence McNamara also points to the need for reform and argues for a streamlined (and general) test for defamatory meaning, but with a different emphasis upon damage to reputation as damage to 'a person's moral status... in the eyes of the community' (McNamara, 2007: 229–232).

The High Court first considered publication in the context of the Internet in the earlier case of *Gutnick*, clarifying the multiple publication approach on the basis that injury was suffered in the comprehension of the defamatory matter, in the jurisdiction where the online material was downloaded or viewed, rather than where it was created. In that decision the majority of the Court usefully stated that:

> Harm to reputation is done when a defamatory publication is comprehended by the reader, the listener, or the observer. Until then, no harm is done by it. This being so it would be wrong to treat publication as if it were a unilateral act on the part of the publisher alone. It is not. It is a bilateral act – in which the publisher makes it available and a third party has it available for his or her comprehension. (Gleeson CJ, McHugh, Gummow and Hayne JJ in *Dow Jones v Gutnick*, 2002, at p. 600)

In the same case Kirby J addressed the specificity of the Internet context for defamation law in some detail, noting the data dimension, and observing that an article published in an online database 'becomes part of the digital collection of data known as a web page' (Kirby J in *Dow Jones v Gutnick*, 2002, at p. 617). His Honour, whilst aware of the need for reform, indicated that this should be undertaken by the legislature and perhaps even take the form of multilateral agreement. While attentive to the characteristics of the Internet and to data-driven forms of publication emerging online, Kirby J adopted a cautious approach in terms of whether wholesale reform was required and, in particular, whether the common law was the right vehicle for such reform. Arguing against technology-specific rules in a common law context, his Honour stated: '[a] legal rule expressed in terms of the Internet might be very soon out of date' (Kirby J in *Dow Jones v Gutnick*, 2002, at p. 631).

Perhaps then in light of the common law's desire for generality in terms of principle and specificity in terms of application (in a fact-sensitive manner), there should be a more robust approach taken to not just who can provide a remedy to those defamed by data association online, but to whether the wide view taken of identification and meaning should be further extended in big data contexts, where meaning derives from indirect association, and where presumably many of us might be unhappy with who or what we might be associated algorithmically. We could ask more pointedly not just whether Google should be a publisher in such contexts, but whether in fact to be defamed by data associations of this nature is to be defamed at all, and to what degree association in the big data environment is to be taken to constitute identification (for a recent decision regarding identification in the online context see *Pedavoli*). This kind of first principles approach can be seen in *Google v Trkulja* 2016 and in *Bleyer v Google* with its reliance on proportionality and case management.

McCallum J's significant decision in *Bleyer v Google* also points usefully to whether defamation by data association in the context of search engines is so stretched in certain cases as to veer towards speculation, and whether having defamation law address these concerns is proportionate to the kind of injury to reputation alleged (*Bleyer v Google*, 2014, at [31]). On this aspect there is an emerging literature in the aftermath of the European decision of *Google Spain* regarding 'the right to be forgotten' which emphasises not the relevance of defamation law to such contexts, but rather data protection laws and the European approach to data protection in particular (Erdos, 2014; Karapapa and Borghi, 2015). It may be the case that despite the common law's willingness to stretch its already wide view of the elements of the cause of action in defamation law to new digital contexts, that over time such contexts may be seen to relate less clearly to the protection of reputation as traditionally understood, and more to statutory data protection with its conceptual roots lying closer to privacy law. This is an emerging trend in some English defamation scholarship which operates against the background of the common law, statutory reform and regional human rights and data protection frameworks (Erdos, 2014).

The broader challenge of big data

Perhaps more significant in the longer term for defamation law, than attempting to apply principles of publication and co-ordinate jurisdictional questions online, will be time spent determining what might be the relevance of our increasing reliance on data associations. This question points to the need to take a wider view of the challenge of digitisation in terms of defamation law's reliance on concepts such as 'community', 'reputation', 'responsibility' and 'identification'. A related policy question emerges: do we now rely on the instantaneous exchange of information to such an extent that the protection of reputation appears to threaten the mechanisms of free speech and freedom of information made possible by the Internet? This latter question is at issue in a significant case decided in the Canadian Supreme Court, *Crookes v Newton*. In that case, the court looked at whether hyperlinks should on their own terms be considered as a form of publication, or whether they were more usefully characterised as a new form of footnote or reference which should not attract liability due to broader interests in the sharing of information and ideas in an information society. The decision is important for its recourse to broader public policy concerns with maintaining a free and open information society. The case is illustrative of a strong, speech-protective approach to determining online liability for defamatory content, which is sensitive to the specific interaction of law and technology in context.

Thus, we can see that the development of the Internet and the turn to reliance on big data gives rise to a range of practical and theoretical questions. Some initial challenges include the following. Do data associations engage defamation principles or are these developments more usefully matched with related areas such as data protection laws or privacy? Where defamation law might be engaged, how is it to interact with these other regulatory forms? Does big data call into question the already rather lite rationale for the protection of reputation in terms of either honour, moral status, dignity, sociality or citizenship (Aplin and Bosland, 2016; Howarth, 2011; McNamara, 2007;

Post, 1986; Richardson, 2013; Rolph, 2008)? Does this transition in fact point to the need to think through the interests at stake differently, perhaps involving more attention to speech, privacy and information flows?

In these terms the challenge and opportunity of big data should see the common law look not only to its pre-existing analytical categories, but also to deeper questions regarding the value of its protections. Viktor Mayer-Schönberger and Kenneth Cukier (2013: 2, 6) write of big data as 'the ability of society to harness information in novel ways to produce insights or goods and services of significant value'. More thought needs to be given as to how this value can be balanced with values such as speech or privacy or reputation, but also whether big data in these terms is communicative in the dialogic sense or more concerned with prediction and problem-solving.

A further challenge lies in how we perceive the rationale for defamation law. Is it to vindicate one's reputation in public as well as to console for hurt feelings, or does it track (in some sense) with a more proprietary conception of reputation as brand or value which relates less to dignity and more to the potential for commodification or celebrity (Rolph, 2008; Varuhas, 2014). For example, in arguing that there is a distinct form of 'reputation as celebrity' David Rolph (2008: 37, 38) has written that reputation 'can be conceptualised not only as a social and an economic construct, but... also as a media construct'.

The reality of the digital archive and its threat of permanence also prompts re-evaluation of the remedy of damages. At the evidentiary level data association promises to specify reputational injury in clearer terms than the law has required. At present the common law presumes damage. Intention is only relevant in terms of defeasance of defences such as comment or opinion and qualified privilege. There has been important recent scholarship which has attempted to analyse and even reformulate the rationale for protection of reputation in the digital context, moving beyond the dated framework of honour (Richardson, 2013) and towards recognition of sociality as underpinning the need to protect against the ostracism involved in damage to reputation online (Howarth, 2011). With human rights frameworks offering a mechanism of balancing by reference to a broader range of interests including speech and privacy, dignity remains an important though rather vague rationale. As Richardson notes, many contemporary instances of online reputational damage 'do not involve false defamatory utterances' (Richardson, 2013: 55).

It may be time to begin thinking differently about defamation, as the example of defamatory data associations (and search engines) suggests. The cases I have examined, illustrate both the sense that this is a developing area where reform and further development of the law may be needed, but also that in many instances the traditional principles are being applied in a pragmatic and orthodox manner, though with mixed and highly fact-specific results. This article has attempted to analyse these developments, but also to point to the need for fresh thinking conceptually. Societal understanding of the significance of reputational damage (and perhaps also the definition of defamatory meaning) is shifting and the commodification and secrecy of reputation management draws into view. As Pasquale (2015a: 14 and see further chapter 2) notes: 'The success of individuals, businesses, and their products depends heavily on the synthesis of data and perceptions into *reputation*. In ever more settings, reputation is determined by secret algorithms processing inaccessible data'. This indicates that while defamation law itself has adapted to the Internet in fairly traditional and predictable ways, it may come to play a central role in regulating the new digital economy. At the very least, this points to a need to give more thought to the suitability of traditional defamation law principles in this emerging context. To this end I have examined a limited category of data association cases involving search engines and algorithmic liability. These cases illustrate some divergence of approaches and a largely pragmatic response to defamation in the context of big data. Such pragmatism needs to be balanced with deeper conceptual analysis and a wider view of the possibility of regulation in this area, where defamation law must increasingly engage with privacy, speech and data protection.

Conclusion

While the big data environment may elude direct relational causality, and threatens at times to overload and disorient, its methods of correlation and association appear to align closely with the breadth of traditional defamation law concepts of publication and identification. The harder question is whether this is desirable. That data associations bring dangers and risk is clear (boyd and Crawford, 2011; Clarke, 2014; Mayer-Schönberger and Cukier, 2013, Chapter 8; Pasquale, 2015b). Defamation law in Australia, and elsewhere, is beginning to consider this in relation to protection of reputation, but it is evident that this forms a small part of what must be a broader development of 'algorithmic accountability' (boyd and Crawford, 2011; Pasquale, 2015b). Within the conceptual terrain of defamation law, as the cases examined illustrate, there should be a wider view taken of what is at stake. In addition to publication and jurisdiction, the courts should give greater weight to the role of identification and to the generation of defamatory meaning in the context of data associations. In looking at how

innocent dissemination is to operate as a defence, a clearer sense of its rationale, rather than its pre-existing technical categories and their applicability will assist. While defamation law may not always be the most suitable regulatory vehicle, it remains a centrally placed one, and in some surprising ways shares much with data associations. Both are 'relational', both engage but also extend further than the terrain of privacy, and perhaps most significantly both rely ultimately on interpretation and the generation of meaning. For defamation law as for big data, it should be remembered as boyd and Crawford (2011: 6) caution, that: 'Interpretation is at the center of data analysis. Regardless of the size of the data set, it is subject to limitation and bias. Without those biases and limitations being understood and outlined, misinterpretation is the result'. This article has focused upon defamation law in Australia as a means of illustrating the broader challenges involved in the governance and regulation of data associations. I have focused on contemporary cases dealing with the liability of search engine operators such as Google Inc for defamatory content. These cases illustrate both the resilience of traditional defamation law principles and their pragmatic use by the courts to determine accountability for algorithmic data association. My focus has largely been upon publication and certain relevant defences such as innocent dissemination. But I have also tried to use the lens of data associations to begin to think differently about domestic systems of defamation law as they grapple with the challenges and opportunities posed by the Internet. These developments point to the need to think more deeply about the value of reputation in these new contexts and for the courts to be more explicit about the underlying function of defamation law in this area.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Aplin TF and Bosland J (2016) The uncertain landscape of Article 8 of the ECHR: The protection of reputation as a fundamental human right? In: Kenyon A (ed.) *Comparative Defamation and Privacy Law* Cambridge: Cambridge University Press, pp. 265–290.

Australian Law Reform Commission (2014) *Serious Invasions of Privacy in the Digital Era*. Report no. 123, 3 September. Canberra: Australian Government.

boyd d and Crawford K (2011) Six provocations for big data (September 21, 2011). In *A decade in internet time: Symposium on the dynamics of the internet and society*, Oxford, UK, 21 September 2011. Oxford Internet Institute. Available at: http://ssrn.com/abstract=1926431 (accessed 14 August 2016).

Clarke R (2014) Big data, big risks. *Information Systems Journal* 26: 77–90.

Descheemaeker E (2009) Protecting reputation: Defamation and negligence. Oxford Journal of Legal *Studies* 29(4): 603–641.

Erdos D (2014) Data protection and the right to reputation: Filling the 'gaps' after the Defamation Act 2013. *Cambridge Law Journal* 73: 536–569.

Howarth D (2011) Libel: Its purpose and reform. *Modern Law Review* 74(6): 845–877.

Karapapa S and Borghi M (2015) Search engine liability for autocomplete suggestions: Personality, privacy and the power of the algorithm. *International Journal of Law and Information Technology* 23: 261–289.

McNamara L (2007) *Reputation and Defamation*. Oxford: Oxford University Press.

Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work and Think*. Boston, MA: Houghton Mifflin Harcourt.

Pasquale F (2015a) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Pasquale F (2015b) Digital star chamber. Available at: https://aeon.co/essays/judge-jury-and-executioner-the-unaccountable-algorithm (accessed 14 August 2016).

Post R (1986) The social foundations of defamation law: Reputation and the constitution. *California Law Review* 74: 691–742.

Richardson M (2013) Honour in a time of Twitter. *Journal of Media Law* 5(1): 45–56.

Rolph D (2008) *Reputation, Celebrity and Defamation Law*. Aldershot: Ashgate.

Rolph D (2010) Publication, innocent dissemination and the internet after *Dow Jones & Co Inc v Gutnick*. *UNSW Law Journal* 33(2): 562–580.

Rolph D (2016) *Defamation Law*. Sydney: Lawbook Co.

Varuhas J (2014) The concept of 'Vindication' in the law of torts: Rights, interests and damages. *Oxford Journal of Legal Studies* 34(2): 253–293.

Australian cases

Bleyer v Google Inc (2014) 88 NSWLR 670

Dow Jones & Co Inc v Gutnick (2002) 210 CLR 575

Duffy v Google Inc [2015] SASC 170

Fairfax Media Publications Pty Ltd v Pedavoli [2015] NSWCA 237

Google Inc v Australian Competition and Consumer Commission (2013) 249 CLR 435

Google Inc v Trkulja [2016] VSCA 333

Radio 2UE Sydney P/L v Chesterton (2009) 238 CLR 460

Thompson v Australian Capital Television Pty Ltd (1996) 186 CLR 574
Trkulja v Google (No 5) [2012] VSC 533
Trkulja v Google Inc [2015] VSC 635
Webb v Bloch (1928) 41 CLR 331

Canadian case

Crookes v Newton, 2011 SCC 47

English cases

Byrne v Deane [1937] 1 KB 818
Garbett v Hazell, Watson & Viney Ltd and Others [1943] 2 All ER 359
Metropolitan International Schools Ltd v Designtechnica Corpn [2011] 1 WLR 1743

European case

Google Spain SL v AEPD, Case C-131/12, 13 May 2014 (Court of Justice of the European Union)

Hong Kong case

Yeung v Google Inc [2014] HKCFI 1404

Legislation

Broadcasting Services Act 1992 *(Cth)*
Defamation Act 2005*(NSW)*

New Zealand case

A v Google New Zealand Ltd [2012] NZHC 2352

This article is a part of special theme on Data Associations. To see a full list of all articles in this special theme, please click here: http://journals.sagepub.com/page/bds/collections/data-associations.